

UNITED STATES DISTRICT COURT
for the
Eastern District of Pennsylvania

United States of America

v.

Andrew Dowdle

) Case No. 18-1217

Defendant(s)

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of 10/9/17 - 7/27/18 in the county of Bucks in the
Eastern District of Pennsylvania, the defendant(s) violated:

<i>Code Section</i>	<i>Offense Description</i>
18 U.S.C. § 2252A(g)	Engaging in Child Exploitation Enterprise.

This criminal complaint is based on these facts:

See attached affidavit.

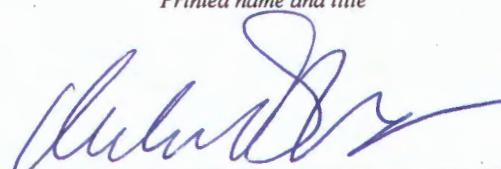
Continued on the attached sheet.



Complainant's signature

Daniel J. Johns, Special Agent, FBI

Printed name and title



Judge's signature

Sworn to before me and signed in my presence.

Date: 07/27/2018

City and state: Philadelphia, Pennsylvania

Hon. Richard A. Lloret, U.S. Magistrate Judge

Printed name and title

AFFIDAVIT

I, Daniel J. Johns, being first duly sworn, hereby depose and state as follows:

1. I am employed as a Special Agent of the Federal Bureau of Investigation (FBI) in Philadelphia, Pennsylvania. I am thus a "federal law enforcement officer," as defined by the Federal Rules of Criminal Procedure. I have been employed as a Special Agent since March 2007. I am presently assigned to the Philadelphia Division's Crimes Against Children squad, which investigates sex trafficking of children and prostitution investigations, child pornography, and kidnappings, among other violations of federal law. I have gained experience through training at the FBI Academy, various conferences involving crimes against children, and everyday work related to conducting these types of investigations.

2. This affidavit is being made in support of the issuance of the attached criminal complaint charging Andrew DOWDLE with engaging in a child exploitation enterprise, in violation of Title 18, United States Code Section 2252A(g).

3. The statements in this Affidavit are based in part on my investigation of this matter and on information provided by other law enforcement officers. Because this affidavit is being submitted for the limited purpose of demonstrating probable cause in support of issuance of the attached complaint, I have not included each and every fact known to me concerning this investigation, but rather only those facts that I respectfully submit are necessary in order to establish probable cause.

STATUTORY AUTHORITY

4. Title 18, United States Code, Section 2252A(g) prohibits any person from engaging in a child exploitation enterprise. In turn, Title 18, United States Code, Section 2252A(g)(2)

provides that a person engages in a child exploitation enterprise within the meaning of the section if the person violates (among other portions of Title 18) Chapter 110 of the United States Code, as part of a series of felony violations constituting three or more separate incidents and involving more than one victim, and commits those offenses in concert with three or more other persons. Chapter 110 of the United States Code prohibits, among other offenses, the production of child pornography (18 U.S.C. § 2251(a)); the advertisement of child pornography (18 U.S.C. § 2251(d)); the distribution or receipt of child pornography (18 U.S.C. § 2252(a)(2)); and the possession of child pornography (18 U.S.C. § 2252(a)(4)(B)). Each of the aforementioned violations is a felony offense.

PROBABLE CAUSE

5. On or about May 23, 2017, an FBI online covert employee (OCE) was investigating the production of child pornography on the mobile app “live.me”¹ and browsed to a website called “8ch.net.” On 8ch.net, the OCE observed a link to an URL permitting browser-based access to Service A, a computer-based communication service described further below. Next to the link was an image that depicted two females who appeared to be children wearing bikinis.

6. The OCE clicked on the above link and was re-directed to another URL to a website operated by Service A. This particular website was entitled “Service A-1,” and the title was accompanied by a thumbnail image of two minor female children kissing each other.

7. Service A owns and operates a free-access all in one voice and text chat application

¹ Live.me is a social media platform for sharing, creating and viewing live streaming videos. Live.me users can stream live video from mobile platforms like Apple iOS or Google Android. Videos streamed from Live.me users can be viewed through the Live.me mobile applications or an internet browser.

and website with the same name that can be accessed over the web. A user creates a Service A account and can then communicate with other Service A users.

8. Service A users can exchange private messages between each other, participate in chat discussions, and voice chat. Service A users can also create chat rooms, which functions as message boards that can be accessed only by Service A users who have an invitation link. Service A-1, mentioned above, is one such chat room on Service A. Within these chat rooms, users can set up different sub-rooms wherein users can type written text, including links to files stored on external file-storage sites, and also upload files under a particular size limit, which can be viewed by all users of the sub-room. Service A users can share files larger than the limit allowed by providing hyperlinks to file sharing websites. Service A chat rooms can have one or more moderators. Moderators have the ability to manage other users, including but not limited to removing users from the chat rooms, elevating users hierarchically, and granting users additional permissions. The moderators of a chat room can categorize users of the chat rooms into hierarchical groups with customized labels and can configure those groups to give users in each group different levels of access.

9. The OCE's review of the Service A-1 chat room revealed that the vast majority of its content consisted of discussions about using web cameras and social-media applications to obtain sexually-explicit images and videos of minor children; images and videos of minor children exposing their vaginas, which at times were uploaded to the Service A-1 chat room and its sub-rooms; and links to download child pornography images and videos from external file-storage sites. Most of the children viewed by the OCE appeared to be approximately between the ages of 11 and 17 years old. The Service A-1 page also included some discussion of adults engaging in sexual activity via web camera. However, the majority of the activity focused on the depiction of

minors engaged in sexually explicit activity on web cameras. For example, in the course of a discussion in the one sub-room of Service A-1 regarding the merits of utilizing virtual private network (VPN) technology to mask users' IP address and identity, Username 1 commented on April 15, 2017: "Just the fact that we're all hanging in here, which is a chatroom where underaged sexual content is shared around is enough reason for one to get a VPN." Username 1 continued,

stating: "Fuck when you download something from dropfile Your ISP can see what you downloaded What if govt authorities read ISPs logfiles." *In the course of the OCE's observations of activity over Service A, at least dozens of users were observed participating in the enterprise described herein, parallel to and in concert with each other, including DOWBLE.*

10. Based on the OCE's undercover observations on Service A-1, a federal search warrant was issued, on or about July 10, 2017, by the Honorable David R. Strawbridge, United States Magistrate Judge, Eastern District of Pennsylvania, for content stored on Service A's servers related to Service A-1. In response to the search warrant, Service A disclosed to law enforcement officers IP address information for some users of Service A-1, the content of some text chats occurring on Service A-1, and some private messages sent by users of Service A-1.

11. The Service A-1 chat room was ultimately shut down by Service A. Members of the Service A-1 chat room proceeded to open additional similar chat rooms on Service A, including: Service A-2, Service A-3, Service A-4, and Service A-5. The OCE gained access to Service A-3, Service A-4, and Service A-5. The OCE observed each of these chat rooms contained many of the same users as Service A-1 and were operated for the purpose of discussing, obtaining, and distributing child exploitation material including child pornography files. Service A-5 is the only of the aforementioned Service A chat rooms that is still operating.

12. Based on the OCE's undercover observations on Service A-2, Service A-3, Service A-4, and Service A-5, a second federal search warrant was issued, on or about November 17, 2017, by the Honorable Linda K. Caracappa, Chief United States Magistrate Judge, Eastern District of

Pennsylvania, for content stored on Service A's servers related to the aforementioned chat rooms. In response to the search warrant, Service A disclosed to law enforcement officers IP address information for some users of those chat rooms, the content of certain text chats occurring in the chat rooms, and some private messages sent by users of those chat rooms.

13. The OCE observed a user of Service A-5 using the online name Username 2 when using Discord. A review of the search warrant return from Discord and undercover recordings by the OCE located the following activity revealed that Username 2 accessed Service A-5 from October 8, 2017, through January 4, 2018.

a. On 10/10/17, Username 2 posted file information uniquely identifying a particular video file on the Service A-5 server. The OCE used the above-described information to download a video file from a video streaming service that depicted a minor female exposing her vagina. The minor child appeared to be between the ages of 12 and 15.

b. On 10/20/17, Username 2 posted different file information uniquely identifying another video file on the Service A-5 server. The OCE used the above-described information to download a video file from the same video streaming service that depicted a minor female exposing her vagina. The minor child appeared to be between the ages of 11 and 14.

c. On 10/23/2017, Username 2 posted different file information uniquely identifying another video file on the Service A-5 server. The OCE used the above-described information to download a video file from the same video streaming service that depicted a minor female exposing her vagina. The minor child appeared to be between the ages of 13 and 16.

d. On 12/15/2017, Username 2 posted a hyperlink to an image file on the Service A-5 server. The OCE clicked on the hyperlink which led to an image that depicted a minor female who appeared to be under the age of 12. The minor female was wearing a shirt, but had

her vagina exposed and her fingers were in close proximity to her vagina.

14. The user “Username 2” also made the following posts on Service A-5 from March 15, 2018, to the present:

a. On June 10, 2018 “Username 2” posted on the Service A-5 server “I’m currently working on my doctorate concerning adolescent behaviors in the online world.” This was in response to other Service A-5 users asking what he and other users were up to. Immediately after Username 2 made that post, Username 5 posted a gif image of a prepubescent child exposing her vagina while urinating. Username 5 followed that posting stating “forgot girls can have tits by watching too many live me vids.”

b. Username 2 posted six live.me video links and three live me user account ID. One of the user accounts appeared to be for a prepubescent minor female.

15. Records disclosed by Discord to law enforcement officers show that user Username 2 accessed Discord servers using 2 particular IP addresses, one from November 18, 2016, to August 7, 2017, and the other on August 22, 2017, October 18, 2017, November 7, 2017, November 9, 2017, December 13, 2017, January 7, 2018, and on at least two occasions per week from February 2018 to June 2018. The FBI served series of subpoenas upon Charter Communications seeking subscriber information for these two IP addresses. The responsive records showed that the subscriber of the first IP address from April 19, 2017 to August 20, 2017, was Andrew DOWDLE, at a particular address in the 100 block of 4th Street, Oswego, NY 13126-2712 with a particular phone number with area code 315. The records also showed that the subscriber of the second IP address from August 22, 2017, to June 29, 2018, was also Andrew DOWDLE, with the same address and phone number.

16. Records disclosed by Discord to law enforcement officers also show that user

Username 2 accessed Discord servers using a third particular IP address on March 15, 2018. Records from Verizon Wireless show that particular IP address was accessed by the same phone number with the 315 area code provided by Charter as associated with subscriber Andrew Dowdle on March 15, 2018.²

17. Username 2 accessed Discord from additional IP addresses during the time period September 2017 to January 2018, but many of these IP addresses returned to Virtual Private Networks (VPNs), and law enforcement is unable to determine their subscribers because VPNs are designed to mask a user's IP address.

18. On July 27, 2018, a federal search warrant was executed at DOWDLE's residence in the 100 block of 4th Street, Oswego, NY 13126-2712. DOWDLE was present at the time the search was executed, and provided a recorded post-Miranda statement to law enforcement officers. In his statement, DOWDLE acknowledged that he was a user of Service A, including both Service A-1 and Service A-5, and further that a search of his computer would yield evidence of the computer's usage by Username 2. DOWDLE acknowledged that he was the owner of the Service A account associated with Username 2, and further provided written consent to the use of Username 2 by law enforcement authorities. DOWDLE further acknowledged that Username 2's login information to Service A was stored in his computer. DOWDLE was shown some of the videos described above. DOWDLE stated that although he did not recognize the particular videos, based upon his typical pattern of usage of Service A, DOWDLE likely would have obtained the videos himself and uploaded them to Service A. DOWDLE further advised that the videos likely

² This IP address is a Natting IP address, meaning that it can be used by several different devices and subscribers. The Verizon Wireless records show that several other phone numbers also used that IP address to connect to the internet on that same day.

were still stored on his digital devices. DOWDLE informed law enforcement officers that hundreds of child pornography files would likely be located by a forensic search of his external hard drive, and that he kept his child pornography files organized. DOWDLE described the purpose of Service A-1 and Service A-5 as to facilitate the dissemination of sexually explicit material depicting “young girls,” the age of whom DOWDLE described as ranging from “preteen to 18.”

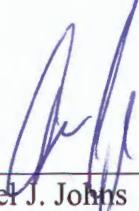
19. Law enforcement officers executing the search warrant at DOWDLE’s residence conducted a forensic preview of the contents of DOWDLE’s digital devices. Located on the hard drive of DOWDLE’s desktop computer were multiple video files depicting minor females apparently between the age of 12 and 17 engaged in the lascivious exhibition of their genitalia, consistent with DOWDLE’s statement regarding the type of material that law enforcement officers were likely to find on his digital devices, including his external hard drive.

VENUE

20. The child exploitation enterprise in which DOWDLE engaged, as described above, extended at all relevant times to the Eastern District of Pennsylvania. The enterprise was open to members from anywhere in the world, and the child pornography material disseminated by the enterprise was made available to any person able to access Service A, including from the Eastern District of Pennsylvania. The OCE’s activities over the various Service A chat rooms comprising the enterprise were conducted in the Eastern District of Pennsylvania. Finally, the investigation has revealed the participation of at least one member of the enterprise who lived in the Eastern District of Pennsylvania and participated in the enterprise from the Eastern District of Pennsylvania, from as early as July 2016 until that member’s arrest by federal authorities in February 2018.

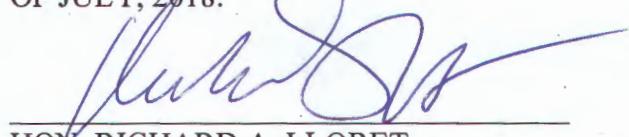
CONCLUSION

21. Based upon the information above, I respectfully submit that there is probable cause to believe that DOWDLE has engaged in a child exploitation enterprise, in violation of Title 18, United States Code Section 2252A(g), in that DOWDLE has violated Chapter 110 of Title 18 of the United States Code as part of a series of felony violations involving three or more separate incidents and more than one victim, and has committed those offenses with three or more other persons. I therefore further respectfully request that the Court issue the attached complaint and warrant charging DOWDLE with that offense.



Daniel J. Johns
Special Agent, Federal Bureau of Investigation

SWORN TO AND SUBSCRIBED
BEFORE ME THIS 27th DAY
OF JULY, 2018.



HON. RICHARD A. LLORET
UNITED STATES MAGISTRATE JUDGE